



Release Notes for the Cisco VPN 5000 Client Software Version 5.2.1

March 8, 2002

These release notes provide information about the Cisco VPN 5000 client software Version 5.2.1. for all operating systems. These release notes are updated as needed to describe new and changed information, caveats, and documentation updates.

This release adds support for the new **ExcludeIPNet** keyword on the VPN 5000 concentrators. For more information see the [“ExcludeIPNet Keyword” section on page 1](#).

Contents

This document contains the following sections:

- [ExcludeIPNet Keyword, page 1](#)
- [Caveats Fixed in This Release, page 2](#)
- [Caveats Fixed in Previous Releases, page 2](#)
- [Open Caveats for the VPN 5000 Client, page 12](#)
- [Limitations for the VPN 5000 Client, page 15](#)

ExcludeIPNet Keyword

This section describes the VPN client support for the **ExcludeIPNet** keyword on the VPN 5000 concentrators.

The new **ExcludeIPNet** keyword on the VPN 5000 concentrators allows you to define a list of IP nets to exclude from a VPN tunnel. If you set this keyword on the VPN 5000 concentrator, the VPN 5000 client reads the data and builds a list of excluded nets. This list allows the VPN client to determine which IP nets are not tunneled.

The VPN 5000 client supports the **ExcludeIPNet** keyword on all operating systems.



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

All VPN 5000 clients that support **ExcludeIPNet** can connect to concentrators that do not support this keyword. VPN 5000 clients that do not support **ExcludeIPNet** can connect to concentrators that support **ExcludeIPNet** only if the keyword is not configured on the concentrator.

Caveats Fixed in This Release

The following sections describe caveats fixed in VPN 5000 client software Version 5.2.1.

Caveats Fixed for Linux

This section describes caveats fixed in VPN 5000 client software Version 5.2.1 for Linux.

- CSCdt51703

The VPN client now creates the necessary folder /etc/Intraport Client/certificates/requests during installation and the “can't open out file” message no longer appears when you attempt to make a certificate request using simple certificate enrollment protocol (SCEP).

- CSCdu50575

When you configure the VPN client for Solaris to exclude local LAN traffic over a PPP connection, local LAN traffic is now excluded from the tunnel.

Caveats Fixed in Previous Releases

The following sections list caveats fixed in previous releases of the VPN 5000 client.

Caveats Fixed for All Windows Platforms

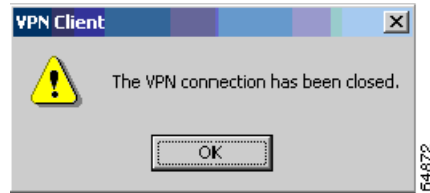
This section lists caveats fixed in previous releases for the VPN 5000 client for all Windows operating systems.

Caveats Fixed in Version 5.1.7

- CSCds39729, CSCdv43326

When the connection from VPN client to the concentrator has been closed, you are notified by a dialog box ([Figure 1](#)). This dialog box does not appear if you exit the VPN client by clicking the **Exit** or **Disconnect** button on the VPN client window.

Figure 1 *Connection Has Been Closed Dialog Box*



- CSCdt79671

A red X appears across the globe in the system tool tray ([Figure 2](#)) when the connection to the concentrator is closed.

Figure 2 *Connection Has Been Closed Indicator*



- CSCdu35956

The documentation has been updated to clarify the installation procedure for preconfigured root certificates in the oem folder.

Caveats Fixed in Version 5.1.1

- CSCdt14207

If you are connected to a concentrator that has the **PFS** keyword in the **VPN Group** section set to any other setting than **Off**, the tunnel now passes traffic.

- CSCdt39202

If the VPN client is connected and closed, and then quickly reopened, a STEP VxD error no longer occurs.

- CSCdu28549

When the client is connected to a secondary server, the VPN client displays the correct server information in the VPN Client window.

- CSCdu71466

The VPN client now writes an exit statement to the VPN session log when you exit the VPN client by right-clicking the globe icon on the tray. Previously an exit statement appeared in the VPN session log if you exited the VPN client using the Exit or Disconnect buttons on the VPN Client window.

Caveats Fixed for Windows 2000

This section lists caveats fixed in previous releases of the VPN client for Windows 2000.

Caveats Fixed in Version 5.1.10

- CSCdv46370
The VPN client now passes traffic when you use it with the Novell client Version 4.8 for Windows 2000 over a dialup or DSL connection.
- CSCdv89432
When you use the VPN client on an IBM Think Pad T22 with an Intel Pro/100 SP NIC, you can now connect to resources and pass data.

Caveats Fixed in Version 5.1.7

- CSCdu71454
The VPN client now properly drops the tunnel when you right-click the globe icon on the system tray and select **Exit**.
- CSCdv31907
When you are using a VPN client configured to use NAT Transparency Mode, the VPN client now disconnects when a VPN concentrator closes the connection.

Caveats Fixed in Version 5.1.1

- CSCdt60740
Large file transfers no longer fail on workstations using the Intel e100bnt5.sys driver shipped with Windows 2000 Service Pack 1.
- CSCdt72278
The WinPoET PPPoE client, Versions 2.0 and 2.1, now initiate connections to upstream PPPoE servers if the VPN client for Windows 2000 is installed on your PC.
- CSCdt81649
The installation process no longer stops and requires user intervention when you select a language other than English during the installation process.
- CSCdu04615
A connection is no longer denied if the VPN client is configured to encrypt passwords, and the concentrator you are connecting to has the **SaveSecrets** keyword set to **True** in the **VPN Group** section.

Caveats Fixed in Version 5.0.12

- CSCdr48602, CSCdr70227
The VPN client for Windows 2000 now supports IPX traffic over dialup connections.

- CSCds14206
When you copy a certificate to the desktop or to the My Documents folder, the VPN client now finds the certificate when you try to import it.
- CSCds48198
The VPN client for Windows 2000 works with Entrust user certificates.
- CSCds80264, CSCdt16845
If you use suspend mode on your workstation, this no longer causes PPP connections to fail or your workstation to crash.
- CSCdt23585
You can now establish multiple tunnels using NAT transparency behind a PIX firewall.

Caveats Fixed for Windows NT

This section lists caveats fixed in previous releases of the VPN 5000 client for Windows NT.

Caveats Fixed in Version 5.0.12

- CSCdr49358
Inconsistent connection attempts no longer occur when you use the Auto-Connect to Default Before Logon option.
- CSCdr86678
The VPN client no longer interferes with the Reflection XTerm display.

Caveats Fixed for Windows ME

This section lists caveats fixed in previous releases of the VPN 5000 client for Windows ME.

Caveats Fixed in Version 5.1.7

- CSCdu11357
You no longer lose Internet connectivity when you install the VPN client for Windows ME on your PC.

Caveats Fixed for Windows 95/98

This section lists caveats fixed in previous releases of the VPN 5000 client for Windows 95/98.

Caveats Fixed in Version 5.1.1

- CSCdv36298

When you end your VPN session using the **Disconnect** button, and close the VPN client window before you click **OK** on the new “The VPN connection has been closed” dialog box, an error message no longer appears. Previously, this only occurred if AutoConnect before Logon was enabled.

- CSCds43082

The VPN client for Windows 95/98 now operates when used in conjunction with AOL Versions 5.0 and 6.0. There are no longer issues with the MaxMTU setting in the registry.

Caveats Fixed for Linux

This section lists caveats fixed in previous releases of the VPN 5000 client for Linux.

Caveats Fixed in Version 5.1.5

- CSCdt46387

When you use the VPN client in active or normal mode FTP, the FTP session no longer locks up if you are using concentrator code that is at or above Version 5.2.21 or 6.0.19. Previously, this problem occurred because the VPN client could not receive traffic through sessions that it did not initiate.

- CSCdt57222

When you use the VPN client with a dialup connection, a certificate in Manual mode no longer fails, and the VPN client can now successfully connect to the concentrator.

- CSCdu33463

When you use the **-n** flag on the command line to use NAT transparency, this no longer overwrites the **UseFTCP=True** keyword in the configuration file.

- CSCdv02607

The keepalive interval on the VPN client push from the concentrator now times out in the correct time frame.

Caveats Fixed in Version 5.1.2

- CSCds56269, CSCdu15222

The **close_tunnel** process no longer fails when you place the **open_tunnel** process into the background and enter your shared secret to receive the "Tunnel open..." message.

- CSCdt42931

The VPN client no longer locks up due to a large number of debugging messages being appearing in the system log.

- CSCdt55349

If you use the VPN client for Linux with RADIUS, SecurID, and a certificate, the SecurID prompt now requests that you enter the Passcode so that a connection can be established.

Caveats Fixed in Version 5.0.19

- CSCdt42931

The VPN client no longer dumps system messages in the debugging log. Previously, a high number of logging messages caused the workstation to lock up.

Caveats Fixed in Version 5.0.8

- CSCdr92677, CSCdt77089

The VPN client using kernel Versions 2.2.5 through 2.2.15 or later no longer causes the operating system to stop responding to console commands.

- CSCds53020

The VPN client now works correctly with a concentrator configured for DNS redistribution.

Caveats Fixed for Solaris

This section lists caveats fixed in previous releases of the VPN 5000 client for Solaris.

Caveats Fixed in Version 5.1.5

- CSCdt78115

When you connect to a VPN group that has the **AutoReconnect** option configured, the VPN client for Solaris now disconnects from the concentrator when it is restarted.

- CSCdt81839

When you use the VPN client for Solaris with a PPP connection in Main mode, the concentrator no longer displays a “WRONG PACKET HERE PAYLOAD=5” message and Error 256. The VPN client no longer times out because the concentrator stops attempting to make the connection.

- CSCdu33463

When you enter the **-n** (fTCP enabled) flag on the command line, you enable NAT Transparency for the active session only and the **UsefTCP** keyword in the configuration is no longer automatically set to **TRUE**. To set all sessions to use NAT Transparency, manually change the UsefTCP keyword in the configuration file.

- CSCdv02607

The VPN client now searches for a lost connection for the proper duration of time before it terminates a connection with a concentrator.

Caveats Fixed in Version 5.1.1

- CSCdt27263

If you use the **mget** command while a VPN tunnel is established, you no longer lose the ability to send packets using FTP.

- CSCdt85193

The VPN client for Intel Solaris no longer becomes inoperable when you attempt to establish a tunnel configured to use NAT transparency. Previously, this occurred using an Ethernet connection with Solaris 8.

- CSCdu30155

Normal VPN client user accounts are now able to communicate with VPN devices over an Ethernet connection.

Caveats Fixed in Version 5.0.11

- CSCdr28631

The Cisco VPN 5000 Solaris client now connects if you have a VPN Group defined without an IPNet value.

- CSCdt09685

If you use an Ethernet connection to establish a VPN tunnel using SPARC Solaris Version 8, the operating system no longer stops working.

- CSCdt52058

The VPN 5000 client for SPARC Solaris no longer tunnels all traffic when using IPNet=0.0.0.0/1.

Caveats Fixed in Version 5.0.8

- CSCds62607

A VPN client for Solaris that is configured to use NAT transparency now encapsulates packets in FTCP for all concentrators.

Caveats Fixed SPARC Solaris

The following caveats have been fixed in the VPN client for SPARC Solaris. They are still known issues in the VPN client for Intel Solaris. See the [“Open Caveats for Intel Solaris” section on page 14](#) for more information.

- CSCdt28570

This problem occurred with Solaris Version 2.6.

When you configure the VPN client for Solaris with interface ipdptp0 over a PPP connection, the client is now able to establish a connection. If you configure the VPN client for Solaris with interface hme2 or -d hme2, you can establish a connection and pass traffic.

- CSCdt51703

During installation, the VPN client now creates the necessary folder /etc/Intraport Client/certificates/requests and a “can't open out file” message no longer appears when you attempt to make a certificate request using SCEP.

- CSCdv29541

When you issue the **close_tunnel** command, the VPN client now searches for a **ps** command to execute instead of executing the first command that resides in the directory defined in the \$PATH variable.

Caveats Fixed for Classic Mac OS

This section lists caveats fixed in previous releases of the VPN 5000 client for the Classic Mac OS.



Note

For information regarding the VPN 5000 Client for Mac OS X, refer to the *Release Notes for the Cisco VPN 5000 Client Software Version 5.2.2 for Mac OS X*.

Caveats Fixed in Version 5.1.2

- CSCdt09734
When an invalid certificate is imported using the Import button on the Certificates tab of the VPN Client window, the client no longer stops working.
- CSCdt73875
The VPN client no longer drops its end of a tunnel after a period of inactivity when connected to a concentrator.
- CSCdu01657
The maximum segment size value for the VPN client has been reduced to 0x0550 (1360) bytes to allow a safety margin for web servers that do not reduce the maximum transmission unit (MTU) of outgoing traffic.
- CSCdu61150
The VPN client now passes packets larger than 1300 bytes when establishing a connection using a Mac PoET PPPoE client from Windriver.

Caveats Fixed in Version 5.0.3

- CSCdr64115, CSCdt29242
The VPN client now manages the TCP MSS value and requires the server to send properly sized packets which can be tunneled from the concentrator to the VPN client.
- CSCds85478
The VPN client now correctly displays the VPN Client window after you close and then reopen it.
- CSCds86954
When a workstation with a VPN client is connected through a tunnel, other local workstations on the network are able to ping the workstation successfully. Although a ping from a local workstation reaches the workstation, any other type of traffic from the local network is silently discarded. There are no IP security issues and it is not detrimental to the IP security or reliability of the VPN client connection.
- CSCds87962
The VPN client will now properly time out a connection attempt to the primary server and roll over to the secondary server if the primary server does not respond.
- CSCds90236
The VPN client no longer attempts to prepare or write debug statements to a file at the improper time.

- CSCdt09163
The message which tells the user to quit all other applications during the installation process has been reworded.
- CSCdt09209, CSCdt09221, CSCdt10158
The readme file has been changed from a text file, which can be modified by the user, to a **ttro** file, which cannot be modified. The release notes in the readme file have also been updated and corrected to remove grammatical errors.
- CSCdt20750
The version number is now included as the first line in the message window of all install programs of the VPN client.
- CSCdt36366
The VPN client Timestamp functions are no longer called at improper times (which causes the VPN client to become inoperable in rare occurrences).
- CSCdt70396
The Mac OS no longer becomes inoperable when the concentrator sends a reset packet back to the VPN client after you have disconnected.
- CSCdt71767
The VPN client now sends the correct minimum version information to the concentrator so that the concentrator can disallow any VPN client that does not meet the **MinimumVersion** variable specified by the VPN Group in the concentrator.

Caveats Fixed in Version 5.0.0

- CSCdr64115
If you use an Apple Directory DA with the VPN client for Mac OS with NAT transparency turned on, this no longer requires that packets be fragmented before you send the packets through the VPN tunnel.
- CSCdr99253
The Macintosh is now able to be placed into Sleep mode so that the VPN client can stay connected to a concentrator.
- CSCdr78540
The RADIUS authentication password dialog box now correctly asks for the password instead of the username.
- CSCds11351
The login dialog window is no longer positioned beyond the visible portion on multiple-monitor configurations. The coordinates of the main window are now checked and adjusted.
- CSCds90274
The VPN client no longer conflicts with the Mac operating system due to debug facilities that remained from previous versions. Previously, this conflict caused the operating system to crash, and Macsbug could not write a standard log when the Mac OS crashed.

Caveats Fixed in Version 4.2.x

- CSCco01093
The VPN client now allows duplicate login names on the Configuration tab of the VPN Client window if the primary servers are different.
- CSCco01132
The shared key entered by a user no longer remains in the VPN client after a failed connection attempt. Each subsequent user is now prompted for a shared key.
- CSCdr30594
An Apple laptop awakening from sleep mode no longer loses its tunnel connection from the concentrator. The VPN client now reestablishes its connections, or quits if it fails to reestablish the connection.
- CSCds11319
The preferences you select in the VPN Client window, such as the window position and column widths, are now saved after you reinstall the VPN client.

The following caveats fixed in Version 4.2.x are not assigned corresponding caveat numbers in the Cisco DDTs.

- The user is now able to select a login from the list on the Configuration tab of the VPN Client window without having the horizontal slide bar in the zero position.
- The vpnsession.log file is now formatted so that it can be easily read by a simple text application.
- User certificates can now be validated against the list of root certificates imported into the VPN client.

Caveats Fixed in Version 3.8.x

The following caveats fixed in Version 3.8.x are not assigned corresponding caveat numbers in the Cisco DDTs.

- When a SecurID login attempt fails or is canceled and there is a secondary server in the login configuration, you now have the option to reconnect, attempt a connection to the secondary server, or cancel.
- You can now store the VPN client files in the Preferences or Extension folders as long as they are located in the System Folder. Also, you are no longer required to keep the System Folder at the root level of the System disk.

Caveats Fixed in Version 3.7.x

The following caveats fixed in Version 3.7.x are not assigned corresponding caveat numbers in the Cisco DDTs.

- You no longer lose the saved shared secret if the VPN client must fail over to the secondary server in your configuration.
- If the primary server in your login configuration does not respond within the allotted time period, you now have a choice to attempt to reconnect or to attempt a connection with a secondary server.
- A default login configuration always exists unless the list is empty, or unless no default entry is specified in the preferences file created by an earlier version of the VPN client.

- The VPN client no longer allows either of the Auto-Connect check boxes on the Configuration tab of the VPN Client window to be enabled if there is no default login configuration specified.
- The VPN client now times out properly and terminates a connection if the concentrator is no longer passing traffic or not responding to the tunnel initiation requests.
- Statistics now properly appear when you use the VPN client with Mac OS Version 9.
- The Tunnel Appletalk check box has been removed from the Configuration tab of the VPN Client window.

Caveats Fixed in Version 3.6.x

The following caveats fixed in Version 3.6.x are not assigned corresponding caveat numbers in the Cisco DDTs.

- The ability to save secrets now works correctly even if the user disconnects in the middle of a connection attempt.
- The VPN 5000 Client Preferences file is now correctly created, accessed, read, and written as long as the folder exists on the Macintosh computer that is running the VPN client.
- If you shut down your computer during an established tunnel connection, the VPN client now closes the tunnel properly.
- A write-to-nil error no longer appears in the Macsbug or Even Better Bus Error applications while attempting to establish a VPN tunnel with a concentrator.
- The VPN client now tunnels DNS packets even when the Exclude Local LAN option is enabled.
- You can now use blank spaces in keywords in the **VPN User** section of the VPN 5000 Client Preferences file.

Caveats Fixed in Version 3.3.x

The following caveats fixed in Version 3.3.x are not assigned corresponding caveat numbers in the Cisco DDTs.

- Problems with editing or adding a new login configuration are resolved.
- The CSC IPAP INIT file no longer causes an error at startup.
- The VPN client now presents a message window to notify you if you lose an established tunnel with the server.

Open Caveats for the VPN 5000 Client

The following sections list known issues for the Cisco VPN 5000 client software Version 5.2.1.

Open Caveats for All Windows Platforms

This section describes open caveats for the VPN client on all Windows operating systems.

- CSCdv43334

If the AutoReconnect feature is enabled, the VPN client does not try to reconnect until you click OK in a dialog box that warns you that the connection has been lost.

No workaround.

- CSCdv70565

If the AutoReconnect feature is enabled in a **VPN Group** that has **SaveSecrets** disabled (the default value), the VPN client does not properly reconnect to the concentrator.

Workaround 1: Enable **SaveSecrets** in the VPN Group.

Workaround 2: Use a user certificate with an embedded **VPN Group** so that both Shared Key and Radius passwords are unnecessary.

For additional security, click the **Advanced** button on the VPN Client window and check the **Encrypt Passwords** box.

Open Caveats for Windows 2000

This section lists open caveats for the VPN client Version 5.2.1 for Windows 2000.

- CSCdu87093

If you install the VPN client for Windows 2000, you might lose the SAP MAPI connections on your computer.

No workaround.

Open Caveats for Solaris

This section lists open caveats for the VPN client Version 5.2.1 for Solaris.

- CSCdv50258

A VPN client for Solaris 8 using the native PPPoE or PPP interfaces fails a connection attempt to a VPN 5000 concentrator because the VPN traffic was not being encrypted before passing through the PPP interface.

No workaround.

Open Caveats for Intel Solaris

The following open caveats apply only to the VPN client for Intel Solaris. These caveats have been fixed in the VPN client for SPARC Solaris. See the [“Caveats Fixed SPARC Solaris” section on page 8](#) for more information.

- CSCdt28570

The following problem occurs with Solaris Version 2.6:

- If you configure the VPN client for Solaris with interface ipdptp0 over a PPP connection, the client is unable to establish a connection.
- If you configure the VPN client for Solaris with interface hme2 or -d hme2, you can establish a connection, but the client does not pass traffic. This problem occurs because the ipdptp stream does not exist when the normal boot time **autopush** command is executed.

Workaround: Manually execute the **autopush** command to allow the ipdptp stream to be created before boot time autopush occurs.

To manually execute autopush:

- a. Create a file named /etc/ppp.ap, which contains the following single line:

```
ipdptp -1 0 vpnmod
```

- b. Obtain superuser privileges.
- c. Issue the following command:

```
autopush -f /etc/ppp.ap
```

- CSCdv29541

The VPN client does not call the full path (for example, /bin/ps) when you issue the **close_tunnel** command. It calls the command that first resides in the directory defined in the \$PATH variable. If another command resides in \$PATH before /bin/ps, the VPN client executes the first command instead.

Workaround: Make sure that /bin/ps is the first directory listed in your \$PATH.

Open Caveats for Classic Mac OS

This section lists open caveats for the VPN client Version 5.2.1 release for Mac OS.

- CSCdu87579

If you are use a VPN client with encrypt passwords disabled and you try to connect to a VPN 5001 concentrator that has shared secrets enabled, the VPN client does not write the shared key to the client preferences file located in the system directory.

Workaround: Delete the system preference file and let the VPN client rebuild it.

- CSCdv85216

You cannot establish SSH connections through the VPN tunnel when you are using a VPN client for Mac OS. However, you can establish SSH connections to an fsecure server if there is no VPN tunnel.

No workaround.

- CSCdw24047

If you are using the VPN client and the system enters sleep mode, the VPN client becomes inoperable and you must reboot the operating system after you awaken your system.

No workaround.

Limitations for the VPN 5000 Client

The following sections list limitations for the VPN 5000 client software Version 5.2.1.

Limitations for All Windows Platforms

This section lists limitations for the VPN client Version 5.2.1 for all Windows operating systems.

- CSCdw32879

The VPN client does not support Token Ring, USB, or PPPoA adapters.

No workaround.

Limitations for Windows XP

This section lists limitations for the VPN client Version 5.2.1 for Windows XP.

- CSCdv78000, CSCdv78304

The VPN client window and dialog boxes do not always appear in the foreground even though you are in an active tunnel session.

Workaround: Double-click the globe in the icon tray to bring the VPN client windows to the foreground.

- CSCdv78110

If you establish a VPN tunnel with an Ethernet connection, subsequent connection attempts over PPP fail if the original Ethernet adapter remains enabled.

Workaround 1: Disable ICMP redirects on the workstation on which the VPN client for Windows XP is installed. To disable ICMP redirects, go to the registry and set the following statement equal to 0:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect.

Workaround 2: Disable the original Ethernet connection using one of the following methods:

- Right-click the icon in the tool tray and choose **Disable** from the menu.
- Enter the **route -f** command from an MS DOS prompt to ensure that all previous caching is removed before you establish the PPP session.



Note If you use the **route -f** command to disable the Ethernet connection, you must manually re-enter the default route for the Ethernet adapter when the PPP session is ended.

- CSCdv80542

If you use the VPN client for Windows XP over a PPP connection, your workstation might become inoperable. This is caused by interference from a service called the QoS Packet Scheduler, which is installed by default with the Windows XP operating system. This problem usually occurs on laptops with internal or PCMCIA modems.

Workaround: Uninstall the QoS Packet Scheduler from your network connection before you use the VPN client for Windows XP.

- CSCdw01856

If you use both the VPN client and Windows Messenger Versions 4.0 and 4.5 on your workstation, you can only pass text traffic and you are unable to use the following features of Windows Messenger:

- White Board
- Audio
- Video
- File Sharing
- Remote Assistance

This limitation is caused by a Network Address Translation (NAT) restriction in the Windows Messenger application.

No workaround.

- CSCdw01873

If you install or upgrade certain networking applications, such as Windows Messenger, the application might be unable to make use of the VPN tunnel.

Workaround: To make sure that the VPN client application recognizes installations and upgrades, you must uninstall and reinstall the VPN client.

- CSCdw01883

If a VPN client user is switched to another account using the Fast User Switching feature of Windows XP, the original VPN tunnel remains active, even though the new account does not have control over the connection and does not know that the connection is active.

Workaround: A VPN tunnel can only be controlled through the account that originally established the tunnel. Before you switch to another account using Fast User Switching, be sure that the VPN tunnel is inactive.

- CSCdw13252

If you use the Remote Desktop feature on a Windows XP Professional workstation, a popup window appears explaining that a VPN5000Gina.dll file is preventing the connection. The VPN5000Gina.dll file is part of the Auto-Connect to Default Before Logon feature of the VPN 5000 client, and the Auto-Connect feature interferes with the remote desktop feature of Windows XP Professional.

Workaround: Disable the VPN5000Gina.dll using the following procedure:

- Open the VPN Client window on your workstation.
- Uncheck the Auto-Connect to Default Before Logon check box.
- Close the VPN Client window.
- Restart your workstation.

Limitations for Windows 2000

This section lists limitations for the VPN client Version 5.2.1 for Windows 2000.

- You cannot install the VPN client for Windows 2000 from a mapped or network drive. You must install the VPN client from a local drive.

- CSCds33439

The VPN client for Windows 2000 displays network errors when used with NetBios traffic.

Workaround 1: To enable local file sharing and printing, set the Local Tunneling Control section of the Advanced Properties dialog box to match the following:

- Tunnel IP = not selected
- Tunnel MS Networking (NetBT) = not selected
- Tunnel IPX = not selected
- Exclude Local LAN from Tunnel = selected
- Exclude DHCP (bootp) from Tunnel = selected

Workaround 2: Disable the Cisco VPN Transport service in the Network Control Panel.

- CSCdt34441, CSCdt36369, CSCdt36383

You cannot use the VPN client for Windows 2000 with a Linksys, Compaq, or Lucent wireless Ethernet configuration.

Workaround: Remove the configuration tool from the Startup menu, and configure the wireless adapter parameters manually in the network properties. If the configuration tool is needed, then the VPN Adapter must be disabled.

- CSCdu47216

If the VPN client for Windows 2000 is installed on your computer and you then install the NetBEUI protocol, this might corrupt your operating system and cause you to reimage your computer.

Workaround: *Before* you install the VPN client for Windows 2000, install the NetBEUI protocol on your computer .

Limitations for Windows ME

This section lists limitations for the VPN client Version 5.2.1 for Windows ME.

- The VPN client for Windows ME does not work with the Novell Client for Netware. Novell does not have a 32-bit client that supports Windows ME.

Workaround: Use the Microsoft Client for Netware with the VPN client for Windows ME.

Limitations for Windows 95/98

This section lists limitations in the VPN client Version 5.2.1 for Windows 95/98.

- Users running Win98-orig cannot connect at startup using vpnautostart.exe when they obtain an address using DHCP. The DHCP lease does not initialize in time for vpnautostart.exe to connect correctly.

Workaround: Update to Windows 98SE, or ensure that all networking updates are applied to the Win98-orig install.

Limitations for Linux

This section lists limitations for the VPN client Version 5.2.1 for Linux.

- The VPN client for Linux does not support Symmetric Multi-processing (SMP) kernels.
- If you configure the VPN client for Linux to use certificates over a PPP connection, local LAN traffic is always excluded, even when your configuration is set to include local LAN traffic.

The VPN client only has control over the interface that is specified for tunneling on the command line. It does not affect other interfaces or devices. For example, if you specify the following command:

```
open_tunnel -d eth1
```

then traffic through eth0 or ppp0, is not affected in any way.

- If you use the VPN client and kernel Version 2.2.x over a PPP connection, large FTP uploads (such as 1 MB) cause the workstation to lock up.

Workaround: Use kernel Version 2.4.x.

Limitations for Solaris

This section lists limitations for the VPN client Version 5.2.1 for Solaris.

- CSCds56269, CSCdv29579

If the `open_tunnel` process is killed using the **kill -9** command, the `open_tunnel` process terminates, but the driver remains in an inconsistent state causing the VPN client to continue tunneling packets.

Workaround: Use the **close_tunnel** command to terminate the `open_tunnel` process and reset the driver.

The following limitation applies only to the VPN client for SPARC Solaris.

- If you configure the VPN client for Solaris to use certificates over a PPP connection, local LAN traffic is always excluded, even when your configuration is set to include local LAN traffic.

Workaround: Set up your routes so that all traffic flows through the PPP interface.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0201R)

Copyright ©2002, Cisco Systems, Inc.
All rights reserved.

